UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/017,368	12/13/2001	Mark S. Moriconi	BEAS-01453US3	8047

23910   7590   06/03/2008

FLIESLER MEYER LLP
650 CALIFORNIA STREET
14TH FLOOR
SAN FRANCISCO, CA 94108

EXAMINER
POLTORAK, PIOTR

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
06/03/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/017,368	MORICONI ET AL.
	Examiner	Art Unit	
	PETER POLTORAK	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9 and 21-31* is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9 and 21-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
      Paper No(s)/Mail Date *3/28/08*.

4) ☐ Interview Summary (PTO-413)
      Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth

   in 37 CFR 1.17(e), was filed in this application after final rejection. Since this

   application is eligible for continued examination under 37 CFR 1.114, and the fee set

   forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action

   has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on

   3/28/08 has been entered.

Response to Arguments

2. Applicant arguments have been carefully considered.

3. In order to address 35 USC § 112 first paragraph rejection, applicant amends the

   claim language and cites paragraph [0087] of the original specification to offer the

   support for the newly added limitation. In particular, applicant suggests that the

   limitations "each application being protected is associated with its own copy of the

   access authorization server" and "the application does not share authorization

   service" have support in following disclosure:

   [0087] The application guard authorization service of the invention imposes virtually no performance overhead on an existing
   application 312. The policy rules developed at policy manager 210 are compiled into an optimized form before being distributed
   to the target application guards 310. This optimized form only distributes attributes relevant to that application guard 310, so
   that access requests may be evaluated by reviewing only a few rules rather than frequently analyzing the potentially large
   policy rule base.

   The examiner is not able to find clear correlation between suggested claim

   limitations and cited paragraph (even when considering neighboring paragraphs),

   and requests a more clear explanation. In particular there are two issues that

   applicant should clearly identify:

- The specification does not identify that "separate applications do not share authorization services",

- The specification does not teach that a system has a plurality of separate application and, more importantly, that "each separate application in the system being protected by its own different copy of access authorization service".

4. Applicant's arguments directed towards Al-Salqan's invention as being an invalid based on the date of the invention is found persuasive.

5. Applicant argues that Donohue teaches the distribution of software updates and patches, which is different from the features of claim 1, specifically "incremental changes relevant to each security engine and computing an accumulated delta that reflects only those changes that are applicable to each different security engine, as defined in claim 1.

   The examiner points out that claim 1, does not include the language argued by applicant, e.g. "each different security engine". However, the examiner points out that Donohue's invention illustrates the fact that distributing changes incrementally (which involves computing an accumulated delta, for example) is not a novel feature, and clearly the choice of updating changes disclosed by Donohue to policies disclosed by Brownlie, either to one or to more security engines would simply be inherent.

6. The remaining arguments are essentially directed towards the newly introduced limitations. These arguments are addressed in this Office Action, below.

7. The text of those sections of Title 35, U.S. Code not included in this action can be

    found in a prior office action.

8. Claims 1-9 and 21-31 have been examined.

Claim Objections

9. Claims 1-9 and 21-31 are objected to because of the following informalities: the

    term "access authorization service" in claim 1 ("… each separate application in the

    system being guarded by its own different copy of access authorization service…")

    lacks the antecedent basis. Similar problem is observed in other independent

    claims.

    Appropriate correction is required.

Claim Rejections - 35 USC § 112

    The following is a quotation of the first paragraph of 35 U.S.C. 112:

10. Claims 1-9 and 21-31 are rejected under 35 U.S.C. 112, first paragraph, as failing to

    comply with the written description requirement. The claim(s) contains subject

    matter which was not described in the specification in such a way as to reasonably

    convey to one skilled in the relevant art that the inventor(s), at the time the

    application was filed, had possession of the claimed invention.

    In particular the original specification does not provide the support for the limitation:

    "each separate application in the system being guarded by its own different copy of

access authorization service such that separate applications do not share

authorization service". See response to applicant arguments, above, for details.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

11. Claims 1-2, 5, 7-8, 21-31 are rejected under 35 U.S.C. 103(a) as obvious over

Brownlie et al. (U.S. Patent No. 6202157) in view of *Donohue (U.S. Patent No.*

6199204).

As per claims 1-2, 5, 7-8, 21-22, 24, 26-27, 29-31 *Brownlie et al.* teach a policy

manager, coupled to a network, including a database for storing a security policy

including a plurality of rules and a policy distributor, coupled to the database, for

distributing the plurality of rules through the network *(Brownlie et al., col. 3 lines 25-*

34, line 54-col. 4 line 2), a security engine located on a client coupled to the network,

for storing a set of the plurality of rules constituting a local customized security policy

received through the network from the policy distributor and for enforcing the local

customized security policy with respect to an application at the client *(Brownlie et al.,*

col. 4 lines 16-43, 51-52 and col. 5 lines 1-5), an application, coupled to the security

engine application rather than being embedded in the application *(Brownlie et al.,*

Fig. 1 node 22, col. 4 lines 47-50 and col. 7 lines 43-49) and the security policy

including a plurality of rules for controlling access to securable objects *(Brownlie et*

al., col. 7 lines 1-22).

12. As per determining incremental changes applicable to the security engine, the

examiner points out that computing environments are subject to constant changes

that are the result of continuing evolution of corporate administrative structure as

well as software advancement.   In addition to ever changing corporate structures as

well as security requirements, software itself evolves (for example it changes and is

replaced) setting new requirements for user interactions.

This notion is also recognized by *Brownlie et al.* who anticipate a series of

incremental changes to a security policy *(Brownlie et al., col. 1 lines 54-56, line 2*

lines 29-30, col. 7 lines 50-54 etc.).

However, *Brownlie et al.* is silent in regard to the specific implementation of

incremental changes to a security policy. Specifically, *Brownlie et al.* do not disclose

that updates involve keeping track of a series of incremental changes, computing an

accumulated delta that reflects the series of incremental changes and sending the

accumulated delta to the subject implementing the changes (the security engine)

from a distributor (the policy manager) such that the subject uses the delta to update

the current setting (the current local customized security policy).

Donohue discloses the process of updating computing systems that involves

keeping track of a series of incremental changes *(Donohue, col. 7 line 59-col. 8*

line10 and Fig. 2) computing an accumulated delta that reflects the series of

incremental changes *(e.g. col. 7 line 66-col. 8 line 2 and col. 9 lines 44-58)* and

sending the accumulated delta to the subject implementing the changes from a

distributor such that the subject uses the delta to update the current setting

(Donohue, col. 4 line 23-28). It would have been obvious to one of ordinary skill in

the art at the time of applicant's invention to compute an accumulated delta that

reflects the series of incremental changes and send the accumulated delta to the

subject implementing the changes from a distributor such that the subject uses the

delta to update the current setting giving the benefit of more efficient updates of

security policies while saving network bandwidth.

(Note that Donohue's invention was used just as an example. However using the

accumulated delta concept is old and well known in the art, see *Flynn et al., (U.S.*

Patent No. 5347653), Nachenberg et al. (U.S. Patent No. 6167407), etc.)

13. Additionally, the examiner points out that the as per keeping track of incremental

changes in network environment it is infeasible to ensure that incremental changes

are implemented by all subjects (clients with security engines) at the same time. For

example, in addition to subjects available for updates, some may be shut down (e.g.

a user taking vacation) and some may not be even in a distributor network (e.g. a

user taking a laptop for a business trip). As a result, comprehensive updates to

already present policy must account for the time difference that results in a different

set of incremental changes distributed to policy subjects. Thus, it would have been

obvious to one of ordinary skill in the art at the time of applicant's invention to keep

track of incremental changes that would allow computation of an accumulated delta

that reflect the series of incremental changes *(for a particular subject)* distributed to

a particular subject given the benefit of a comprehensive update of each subject

using a minimum of network bandwidth and a flexible update schedule.

14. Furthermore, there are essentially only a few possibilities to update current

configuration (such as policies) in order to reflect the most current desirable state

(the most current overall configuration), which could include multiple intermediate

updates. The newest most current overall configuration settings could be used to

overwrite the current configuration. The changes could be implemented gradually, or

only the difference (delta) between the current and most updated overall

configuration could be installed. (The last one reads on the claimed limitations) Any

of these implementations, are obvious variations of each other. However, taking in

consideration time and network bandwidth required to deliver and update all network

subjects, the delta implementation would have been the most obvious choice.

Transferring less data via network minimize the use of the network bandwidth and

less data to install speeds up the update process and minimize possibility of errors.

15. **As per newly introduced limitations,** although in Fig. 1, *Brownlie et al.* discloses

only one set of a security engine/application being guarded by a copy of access

authorization service set, Brownlie clearly discloses that there may be more than

one client 22 (thus, more than one set of a security engine/application being guarded

by a copy of access authorization service). Specifically, Brownlie teaches that "the

system 10 also includes a plurality of network nodes 22 that have access to the

public directory 20 through a network link 24" (col. 4 lines 16-18). Clearly,

applications on different clients read on separate applications and by virtue of

residing on different clients that have different security engines, these separate

applications clearly do not share the same authorization services.

16. As per claims 25 and 29 *Brownlie et al.* changes inherently include one or more of

adding, deleting and amending.

17. As per claims 22-23 and 27-28 the table disclosed by *Donohue* in Fig. 2 reads on a
policy tracking table. Furthermore, Official Notice is taken that it is old and well-
known practice to store data in a table and using the stored data in reconstruction of
a computer systems to a previous state. It would have been obvious to one of
ordinary skill in the art at the time of applicant's invention to reconstruct a computer
state to the previous version using earlier stored and distributed data given the
benefit of a quick troubleshooting of problems, potentially introduced by the data.

18. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Brownlie et
al. (U.S. Patent No. 6202157)* in view of *Donohue (U.S. Patent No. 6199204)* and
further in view of *Wang (U.S. Patent No. 5956521).*
Brownlie et al. discloses that the policy manager and the policy distributor are hosted
on a first server *(Brownlie et al., col. 3 lines 27-34, 54-56 and 61-63)*, the security
engine and the application are hosted on a second node, and the first and second
node are communicatively coupled to each other through the network *(col. 3 lines
61-63).*

19. *Brownlie et al.* do not explicitly teach that the second node is a server.
Wang teach a plurality of nodes that are servers *(Wang, Fig. 3).*
It would have been obvious to one of ordinary skill in the art at the time of applicant's
enforceable security policy invention as disclosed by *Brownlie et al.* into systems
with nodes that are servers as taught by *Wang*. One of ordinary skill in the art would

have been motivated to perform such a modification in order to provide an

enforceable flexible security policy for each network node including servers.

20. Claims 3-4 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Brownlie et al. (U.S. Patent No. 6202157) in view of *Donohue (U.S. Patent No.*

6199204) and further in view of *TRCKA et al. (U.S. Pub. No. 20010039579)* and

Microsoft Press (Computer Dictionary, 3rd Edition, ISBN: 157231446XA, 1997).

Brownlie et al. disclose the security engine as discussed above.

As per claims 3 *Brownlie et al.* teach the security engine for evaluating a request to

access the application based on the set of the plurality of rules and the application

and the engine to communicating *(Brownlie et al., col. 4 lines 47-50 and col. 7 lines*

43-49).

21. *Brownlie et al.* do not explicitly teach an application programming interface (API) for

enabling communication between the application and the engine.

TRCKA et al. teach utilizing API in communication *[101].*

It would have been obvious to one of ordinary skill in the art at the time of applicant's

invention to provide API for enabling communication between the application and the

engine as taught by *TRCKA et al.* One of ordinary skill in the art would have been

motivated to perform such a modification in order to code efficiency by allowing

significant amount of code to be re-used *[103].*

22. *Microsoft* teaches a plug-in *(Microsoft Press, pg. 370).*

It would have been obvious to one of ordinary skill in the art at the time of applicant's

invention to incorporate a plug-in API as taught by *Microsoft.* One of ordinary skill in

the art would have been motivated to perform such a modification in order to provide

additional functionality *(Microsoft, pg. 410)*.

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Peter Poltorak whose telephone number is (571) 272-

3840. The examiner can normally be reached Monday through Thursday from 9:00

a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number

for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

/Peter Poltorak/

Examiner, Art Unit 2134

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2134